WHAT IS CLAIMED IS:

1   1.   A method comprising:

2   in a server, hosting an intrusion detection process that

3   provides intrusion detection services; and

4   integrating the intrusion detection process with a server

5   process.

1   2.   The method of claim 1 in which integrating comprises:

2   defining global application programmer interface (API)

3   structures in the intrusion detection process to establish a

4   connection to an application programmer interface (API) of the

5   server process.

1   3.   The method of claim 2 further comprising:

2   passing a request for data received by the server to the

3   intrusion detection process.

1   4.   The method of claim 3 in which the intrusion detection

2   process comprises:

3   packing a subset of the data into an analysis format; and

4   passing the subset to an analysis process.

1   5.   The method of claim 4 further comprising analyzing the

2   subset in the analysis process.

1   6.   The method of claim 1 in which the server is a web

2   server.

1   7.   The method of claim 6 in which the web server is an

2   Apache web server.

1   8.   The method of claim 4 in which the analysis process is

2   resident in the web server.

1   9.   The method of claim 4 in which the analysis process is

2   resident outside of the web server.

1   10.   The method of claim 4 in which passing further comprises

2   delivering the subset in a funneling process via a socket.

1   11.   The method of claim 10 in which the funneling process

2   comprises:

3   accepting incoming connections to which the subset can be

4   transmitting; and

5   passing the subset to outgoing connections.

1   12.   A method comprising:

2   passing a request for data received by a first server

3   process executing in a first server to a detection process

4   that includes:

5   packing a subset of the data into an analysis format; and

6   passing the subset to an analysis process.

1   13.   The method of claim 12 also including

2   analyzing the subset in the analysis process.

1 14. The method of claim 12 in which passing comprises passing

2 control from the first server through an Application

3 Programming Interface (API) of a server program.

1 15. The method of claim 12 in which the first server

2 comprises a web server.

1 16. The method of claim 12 in which the detection process is

2 resident in the first server.

1 17. The method of claim 13 in which the analysis process is

2 resident in the first server.

1 18. The method of claim 13 in which the analysis process is

2 resident in a second server.

1 19. The method of claim 12 in which the analysis format

2 comprises an Emerald format.

1 20. The method of claim 12 in which the analysis process

2 comprises an Emerald eXpert analysis process.

1 21. The method of claim 15 in which the web server comprises

2 an Apache web server.

1 22. The method of claim 21 in which the passing further

2 comprises:

3   receiving the subset in a piped logs interface of the

4   Apache web server; and

5   delivering the subset to a funneling process via a

6   socket.

1   23.   The method of claim 22 in which the funneling process

2   comprises:

3   accepting incoming connections to which the subset can be

4   transmitted; and

5   passing the subset to outgoing connections.

1   24.   The method of claim 22 in which the funneling process

2   further comprises duplicating the subset for delivery to a

3   second analysis process.

1   25.   A system comprising:

2   a web server process having an application programming

3   interface (API); and

4   an intrusion detection process linked to the API.

1   26.   The system of claim 25 further comprising a link to an

2   external system having an analysis process.

1   27.   The system of claim 26 in which the intrusion detection

2   process comprises:

3   receiving a request for data;

4   packing a subset of the data into a common analysis

5 format;

6   passing the subset to the analysis process; and

7   analyzing the subset in the analysis process.

1 28.   The system of claim 25 in which the web server process is

2 an Apache web server process.

1 29.   The system of claim 26 in which the common analysis

2 format is an Emerald format.

1 30.   The system of claim 26 in which the analysis process is

2 an Emerald analysis process.

1 31.   A computer program product residing on a computer

2 readable medium having instructions stored thereon which, when

3 executed by the processor, cause the processor to:

4   receive a request for data;

5   pack a subset of the data into a common analysis format;

6   pass the subset to an analysis process; and

7   analyze the subset in an analysis process.

1 32.   A processor and a memory configured to:

2   receive a request for data;

3   pack a subset of the data into a common analysis format;

4   pass the subset to an analysis process; and

5   analyze the subset in an analysis process.

1   33.   A computer program product residing on a computer

2   readable medium having instructions stored thereon which, when

3   executed by the processor, cause the processor to:

4   integrate an intrusion detection process with a server

5   process.

1   34.   A processor and memory configured to:

2   integrate an intrusion detection process with a server

3   process.